

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

RAJENDRASINH BABUBAHAI
MAKWANA,

Defendant

CRIMINAL COMPLAINT

Case No.:

UNDER SEAL

09 0011 PWG

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about October 24, 2008, in the District of Maryland, the defendant,

RAJENDRASINH BABUBAHAI MAKWANA,

knowingly caused the transmission of a program, information, code, and command and, as a result of such conduct, intentionally and without authorization caused and attempted to cause damage to a protected computer, and by such conduct caused and would have caused damage affecting a protected computer system used by and for victim company "ABC" that is, RAJENDRASINH BABUBAHAI MAKWANA embedded a malicious code in pre-existing "ABC" software that was intended to execute on January 31, 2009, at which time it would have destroyed the "ABC" data on approximately 4000 servers and obliterated the evidence of the embedding of said malicious code, in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(b), 1030(c)(4)(A), and 2.

I hereby certify that I am a Special Agent with the Federal Bureau of Investigations, and that the facts upon which this complaint is based are as follows:

SEE ATTACHED AFFIDAVIT

continued on the attached page and made a part hereof..

Sworn to before me and subscribed in my presence,
on this 6 day of January, 2009, in Baltimore, Maryland

HONORABLE PAUL W. GRIMM
UNITED STATES MAGISTRATE JUDGE

Jessica A. Nye
Jessica A. Nye, Special Agent, FBI

Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND

UNITED STATES OF AMERICA)

v.)

RAJENDRASINH BABUBHAI)
MAKWANA,)

Defendant.)

CRIMINAL NO.

UNDER SEAL

09 0011 PWG

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT
AND ARREST WARRANT

I, Jessica A. Nye, being duly sworn, depose and say:

I. INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation and have been so employed since March 19, 2006. I am presently assigned to the Baltimore Field Office, where I investigate Computer Intrusions, Cyber Threats, Internet Fraud, and Crimes Against Children. I have received training in general law enforcement, and in specialized areas including computer science, cyber investigations, and crimes committed utilizing computers and computer networks, such as hacking, denial of service attacks, and malicious code. I have participated in criminal investigations involving hacking, malicious code, botnets, spamming, and threats.

2. This investigation involves violations of Title 18, United States Code, Section 1030(a)(5)(A) which prohibits in pertinent part knowingly and willfully attempted to cause the transmission of a program, information, code, and command and as a result of such conduct, intended to cause damage without authorization to a protected computer, that is, one which was used in interstate commerce and communication, and by such conduct, if completed, would have caused loss to one or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value.

3. The information contained in this affidavit is known personally by me as a result of my direct participation in the investigation; from interviews of persons referenced in this affidavit; from the review of business records; from the review of computer logs; and from my conversations with other agents and law enforcement officers.

[Handwritten signature]

[Handwritten initials]

4. I submit this affidavit for the limited purpose of establishing probable cause in support of this application for a criminal complaint, and thus, it does not contain every fact gathered during the investigation. Additionally, unless otherwise noted, wherever in this affidavit I assert that an individual made a statement, that statement is described in substance, and in part, and is not intended to be a verbatim recitation of the entire statement.

II. SUBJECT

5. RAJENDRASINH BABUBHA^I MAKWANA ("MAKWANA") is the subject of this investigation. MAKWANA is a thirty-five year old male and a native citizen of India. He currently resides in Frederick, Maryland on a work Visa. I have confirmed his personal identification information through the Maryland Motor Vehicle Administration, public and private databases.

III. RELEVANT STATUTES

6. Title 18, United States Code, Section 1030(a)(5) provides :

Whoever –

* * * * *

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

* * * * *

(B) by conduct described in clause (I) . . . of subsection (A), caused (or, in the case of an attempted offense, would, if completed, have caused) (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

* * * * *

shall be punished as provided in subsection (c) of this section.

IV. COMPUTER TERMS AND GENERAL DEFINITIONS

7. Internet Protocol (IP) – IP addresses are unique and are represented by 4 groups of numbers separated by periods. They identify specific computers on the Internet or on an internal network. (i.e. 160.111.7.240 is the Smithsonian).

8. Server – A computer in a network shared by multiple users. A server is a high-speed computer in a LAN that stores the programs and data files shared by users on the network.

09 0011 PWG

9. Unix – A type of computer operating system. The Unix operating systems can be used in both servers and workstations.

10. Root Access – In Unix computer operating systems, root access is the conventional name of the user who has all rights or permissions.

V. PROBABLE CAUSE

11. “ABC” is a pseudonym for the victim company, which is a publicly traded United States company in the mortgage business. ABC has a nationwide presence working with other mortgage bankers, brokers, and primary mortgage market partners. They have a nationwide internal computer network, including about 4,000 computer servers, that supports their mission. They have branch offices throughout the country, and have a data center in Urbana, Maryland at which the target of this affidavit was employed.

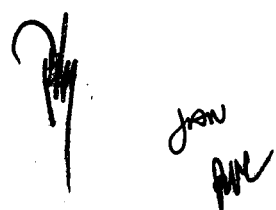
12. As of October 24, 2008, MAKWANA was a OmniTech employee. He had been working under contractor at ABC for approximately three years as a Unix Engineer at ABC’s Urbana, Maryland facility. He was proficient in the Unix computer language designed to operate computer servers. MAKWANA was part of the common operations group within ABC that created computer scripts for ABC. He had root access to ABC servers, giving him full access to the ABC servers.

13. On October 24, 2008, between 1:00 and 1:30 p.m., MAKWANA, was terminated as a contractor working for ABC. He was terminated because on or about October 10th or 11th, 2008, MAKWANA erroneously created a computer script that changed the settings on the Unix servers without the proper authority of his supervisor. This computer script was not maliciously created. After this incident, MAKWANA was able to continue to work on computer scripts but was not allowed to push the computer scripts out on ABC servers.

14. When MAKWANA was told it was his last day with ABC, by a ABC manager, he did not seem surprised. MAKWANA emailed OmniTech at approximately 2:00 p.m., advising them of his termination. Between 2:00 and 2:30 p.m., MAKWANA was told that all of his ABC equipment to include his badge, laptop, etc., needed to be turned in by the end of the day. The procurement department of ABC contacted OmniTech to let them know of MAKWANA’s termination.

15. MAKWANA’s last recorded activity on his ABC laptop occurred at approximately 4:30 p.m. At approximately 4:45 p.m., MAKWANA dropped off his badge and laptop to a ABC employee.

16. Despite MAKWANA’s termination, MAKWANA’s computer access was not immediately terminated. Access to ABC’s computers for contractor’s employees was

Handwritten signature and initials in the bottom right corner of the page.

09 0011 PWG

controlled by the ABC procurement department, which department did not terminate his MAKWANA's computer access until late in the evening on October 24, 2008.

17. On October 29, 2008, SK, an ABC senior Unix engineer, discovered malicious script embedded within a pre-existing, legitimate script. This legitimate script runs every morning at 9:00 a.m. validating that there are two storage area network paths running correctly and operationally through all ABC servers.

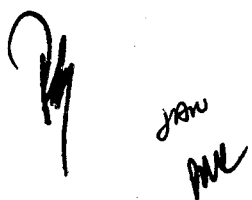
18. The malicious script was at the bottom of the legitimate script, separated by approximately one page of blank lines, apparently in an effort to hide the malicious script within a legitimate script. It was only by chance that SK scrolled down to the bottom of the legitimate script to discover the malicious script. The legitimate and malicious script were removed and placed into an archive file on October 29, 2008.

19. SK and his supervisors ordered a standard lock down of all access to the servers to determine if any other malicious script was present and to determine who created the malicious script. This malicious script was created on the development server, *dsysadm01*, and would execute from the production server, *psys-tr-adm01a*. The legitimate script in which the malicious code was embedded was a script located on the *psys-tr-adm01a* server. There are only approximately ten to twenty ABC employees and contractors, to include MAKWANA, that had access to the *psys-tr-adm01a* server. SK immediately looked at the logs from October 24, 2008, the date of the creation of the malicious script, and noticed MAKWANA's username and files accessing the *dsysadm01* server, on which the malicious script was created.

20. SK and other system administrators were able to preserve the production and development servers as well as the logs accessing these servers. These restored copies copied the data and settings of the servers on October 21, 2008 before the attack and a day after the attack on October 25, 2008, to show the changes made to the server prior to SK finding the malicious script.

21. On October 24, 2008 at 2:53 p.m., a successful SSH (secure shell) login from IP address 172.17.38.29, with user ID s9urbm, assigned to MAKWANA, gained root access to *dsysadm01*, the development server. This IP address is an ABC assigned IP address assigned to specific computers used within the ABC network. IP address 172.17.38.29 was last assigned to the computer named rs12h-Lap22, which was an ABC laptop assigned to MAKWANA. There are logs at ABC that periodically send reports of changes of computer ownership, which has not occurred for rs12h-Lap22 since at least July 2008. This is the same laptop that MAKWANA turned in at approximately 4:45 p.m. The laptop and the Unix workstation where MAKWANA was able to gain root access and create the malicious script were located within his cubicle.

22. Internet access for end-user computers at ABC must pass through a proxy, which requires a unique username and password. ABC employees and contractors are prohibited from sharing their password. ABC Websense logs show that user ID s9urbm

Handwritten signature and initials in the bottom right corner of the page.

09 0011 PWG

conducted authenticated web browsing from the IP address 172.17.38.29 between 3:01 p.m. and 3:32 p.m. on October 24, 2008. The proxy logs additionally indicate that user ID s9urbm had been using the same IP address since at least October 20, 2008. A typical lease time for end-user IP address assignments at ABC is five days, and then a computer would request renewal of the same address.

23. Upon gaining root access on October 24, 2008, MAKWANA created a directory called ".soti." The file entitled ".soti" was not present on October 21, 2008 as seen on the restored copy of the server, but was seen on the restored copy of the server on October 25, 2008. Further examination indicates that the ".soti" file contains the files that were created to execute the malicious script to include: .x.sh, .y.sh, .spa, .z.sh, .a.sh. The log entries show continued activity where the user s9urbm created and edited the script files, to include .x.sh, .a.sh. and .y.sh, later discovered to contain destructive routines.

24. This malicious script did not execute because it was set to run on January 31, 2009. Because it was embedded within a legitimate script that automatically ran every morning at 9:00 a.m., this script would begin to run but when the program realized it was not January 31, 2009, it would stop running and not fully execute.

25. If the malicious script had executed from the *psys-tr-adm01* server, it would copy the .x.sh file from the *dsysadm01* server which begins by checking the date to determine if the script should execute. When the program ascertained it was January 31, 2009, it would copy the rest of the files from the ".soti" file from the *dsysadm01* server and run the .y.sh script. The .y.sh script would place a blocker on the monitoring system disabling any ABC engineers from receiving a monitoring alert for any problems on any machines in the entire ABC environment for 61 minutes. The ABC engineers would ordinarily receive such an alert. In addition, the script would build a list of all servers within ABC and also disable all logins to the *psys-tr-adm01a* server and the backup production server, *psys-tr-adm01z*, so that no one could login to these servers.

26. The script would then run .z.sh which would create a list of production, contingency, and backup servers and then run .a.sh on all of ABC servers. Script .a.sh would disable all logins and clear out all logs, including all the logs that revealed MAKWANA's access to the *dsysadm01* server on October 24, 2008 thus eliminating his "footprints." If a ABC engineer attempted to login a message "Server Graveyard" would be displayed. This script would also remove the root password appliance access to the server by updating the password and shadow files so no one could change the root password from the password appliance. Next .a.sh would build a list of all servers that contain ABC data and wipe out all of the data and replacing the data with zeros. This would also destroy the backup software on the servers making the restoration of data more difficult because new operating systems would have to be installed on all servers before any restoration could begin. The script would also remove all "High Availability" software from any critical server. And finally this script would power off all servers, disabling the ability to remotely turn on a server. Subsequently, the only way to turn the

JAN
me

servers back on was physically getting to a datacenter to turn the servers back on. This script would propagate itself out to all 4,000 ABC servers, thus damaging all ABC data.

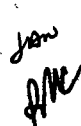
27. Once this script ran, it would run the same script from server *psysadm02* in case some of the servers could not be reached from *psys-tr-adm01a*. After the second run through, the script would remove all the files on the current host and try to zero out the root file system.

28. According to ABC engineers, MAKWANA's laptop showed similar naming schemes of his temporary files, for example he named his temporary files: .x and .p. This nomenclature is very similar to the naming schemes of the malicious script, for example .x.sh. This is not the typical nomenclature a Unix engineer would use.

29. Any ABC data that was not restored prior to this malicious script executing would be lost. Approximately one week after the October 24, 2008 incident, all 4,000 ABC servers and all legitimate scripts were checked twice to ensure that no other malicious scripts were present on their network. ABC engineers have restored the legitimate script that contained the malicious script to function correctly. The expenses incurred from this response have exceeded \$5,000.00. Had this malicious script executed, ABC engineers expect it would have caused millions of dollars of damage and reduced if not shutdown operations at ABC for at least one week. If this script were executed, the total damage would include cleaning out and restoring all 4,000 ABC servers, restoring and securing the automation of mortgages, and restoring all data that was erased.

30. After discovery of the malicious script, ABC reviewed MAKWANA's emails a few days before the creation of the malicious script and on his last day. In one email, MAKWANA communicated to his relatives in India instructing them not to return to the United States.

31. Based on the above conduct, that RAJENDRASINH BABUBHA~~I~~ MAKWANA intentionally created a malicious script that would execute three times to ensure the removal of all ABC data on ABC servers and such data replaced with zeros, there is probable cause to believe that RAJENDRASINH BABUBHA~~I~~ MAKWANA has violated Title 18, United States Code, Section 1030(a)(5).



09 0011 PWG

VI. CONCLUSION

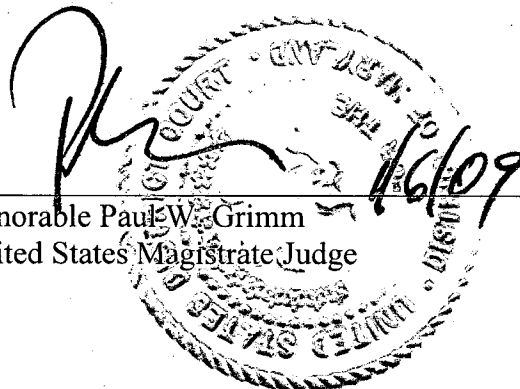
32. Based on the foregoing, I respectfully submit that there is probable cause to believe that RAJENDRASINH BABUBHAMAKWANA has violated Title 18, United States Code, Section 1030(a)(5) and request a criminal complaint and arrest warrant for RAJENDRASINH BABUBHAMAKWANA be issued.

The abovementioned is true and correct to the best of my knowledge, information, and belief.

Jessica A. Nye 1/6/09
Jessica A. Nye, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me
this _____ day of January 2009.

[Signature] 1/6/09
Honorable Paul W. Grimm
United States Magistrate Judge



[Handwritten signature]

[Handwritten signature]